EXECUTIVE COMPUTING

HILLEL SEGAL

Safeguard your business against computer crime

IS IT REALLY necessary for small computer owners to worry about computer crime? Absolutely. Any business which relies on computers to pay bills, issue payroll checks, inventory merchandise or perform normal accounting functions is vulnerable to computer theft.

Sad to say, the most common culprit is a trusted employee — and this person is frequently "tempted" to cheat by the *lack* of simple security procedures.

There's nothing new about the methods of computer fraud. For the most part, today's criminals use age-old embezzlement methods, but they do them faster and better with the help of computers. Fraudulent bookkeeping entries are far easier to hide with a computer than old fashioned book-juggling. Changes in handwritten books arouse suspicion, but entries in a computer's files can often be made without detection.

It's a serious problem

In short, without the proper safeguards, a small computer can make embezzlement easier to accomplish and harder to detect. With manual systems, only a few employees have access to the books and have an opportunity to defraud. With automation, it is common for many people to have access to the accounting records.

The most frequent type of security loss involves the manipulation of funds: diverting payments to suppliers, adding payroll checks for phantom workers, skimming receipts by recording sales at a discount when the customer actually paid full price.

With these types of schemes in mind, the small, unguarded computer can put a low-paid person in a position to steal enough money to bankrupt a business. Unlike larger mainframe computers, smaller systems typically do not have built-in control procedures, nor the management staff familiar with these types of

risks. A common attitude is "Let's get the system working and worry about security later," or "It can't happen here."

These points of view, unhappily, can lead to an undisciplined computer environment that is ripe for trouble.

The solution lies in low-cost security measures like the ones I'll suggest. These techniques depend largely on prevention. They can be established without great expense and, in most cases, without technical assistance.

The goals of these measures are to **1.** protect company assets; **2.** protect the privacy of sensitive data; **3.** keep employees from unnecessary temptation; **4.** deter employees who have the opportunity to defraud and **5.** discover problems if they occur.

Computer security techniques

Here's how to begin:

✔ Control access to the computer. The most basic form of security is control over who has access to the machine. For small businesses, this is one of the simplest and most effective deterrents to computer crime. It can be accomplished with separate computer rooms, avoidance of auto-answer modems (devices permitting easy access to the computer by telephone) and use passwords that are changed regularly.

✔ Rotate the jobs and responsibilities of employees who use the computer. This allows more than one person to learn each task, providing the added benefit of backup in case of illness or termination. Sometimes it's best not to announce the actual date of each rotation until the last minute. In this way, it acts as a deterrent because employees will not know when they may have to leave their present position and be unable to "cover their tracks."

✔ Purchase computer insurance (such as the policy available through the Association of Computer Users) that specifically covers against computer fraud. Such insurance is better than bonding because it covers all employees, not just the ones bonded.

✔ Insist that all personnel having access to the computer take a vacation each year. Embezzlers may decline vacations because their constant efforts are needed to avoid detection, so get suspicious if you notice vacation-avoidance behavior.

✔ Spot-check regularly. Look at the list of accounts payable. Are there any unfamiliar names? Did you actually receive the merchandise? A short time spent browsing through payroll or accounts-receivable records can turn up past misdeeds and discourage future attempts. As a deterrent, be sure that employees understand that their work is subject to unannounced checking at any time.

✔ If you don't have the time to take these kinds of security measures seriously, call in an outside expert or your accountant to do it for you. For a fee ranging from $1,000 to $2,000 they can conduct checks and set up procedures that might save you much more than that in the long run.

✔ Finally, do what most professional data processing managers insist on: conduct an annual security audit. Nothing is better to impress upon your staff the importance of security. Over time, employees gradually become less alert and less committed to security, and periodic audits accompanied by briefings will help motivate your staff to comply.

Hillel Segal is an independent computer consultant and editor of the Executive Computing Newsletter, published by the Association of Computer Users. He can be reached at ACU, P.O. Box 9003, Boulder 80301.